UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,700	01/18/2001	Ashok Vadekar	06944.0033	4704

27871 7590 01/27/2005

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application N .	Applicant(s)	
	09/761,700	VADEKAR ET AL.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 August 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9 are pending in this application and have been examined.

Drawings

2. The drawings were received on 8-24-2004. These drawings are not acceptable. In order to avoid abandonment, the drawing informalities noted in the paper mailed on 2-20-2004, must now be corrected. Correction can only be effected in the manner set forth in the above noted paper.

Claim Objections

3. Claim 6 is objected to because of the following informalities: The preamble should read "A method of performing a selected group *operation*... Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "substantially" in claim 1 is a relative term that renders the claim indefinite. The term "equal" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably appraised of the scope of the invention.

Claims 2-5 are dependent on claim 5 and are thereby rejected on the same basis.

Claim Rejections - 35 USC § 101

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1-9 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As for claim 1, the claim is directed towards non-statutory subject matter. It is not apparent from the preamble of the claim: "A method of determining a result of a group operation performed on a computing apparatus..." that the claim language is directed towards any type of relationship between a result calculated on a computing device and any subject matter outside the device that constitutes the invention. (See MPEP 2106[R-2]-2106.02). As such the claim language is directed to a process that consists solely in the manipulation of data or an abstract idea that is not concrete or tangible. No benefit in efficiency or other characteristic to the computing device is asserted in the preamble, nor any use for the data so manipulated. It is not clear that the claimed

method is embodied in a memory medium that, when read out by the computing device, consists of a series of steps executed by the computer, or if the method is merely performed manually by human input to a keyboard for example.

As for claim 6, the claim is directed towards non-statutory subject matter. It is not apparent that the claim language is directed towards any type of relationship between a result calculated on a computing device that is a crypto processor, and any subject matter outside the device that constitutes the invention. (See MPEP 2106[R-2]-2106.02). As such the claim language is directed to a process that consists solely in the manipulation of data or an abstract idea that is not concrete or tangible. No use for the data so manipulated is asserted. It is not clear that the claimed method is embodied in a memory medium that, when read out by the computing device or crypto processor, consists of a series of steps executed by the computer, or if the method is merely performed manually by human input to a keyboard for example.

Claims 2-5, and 7-9 are dependent on claims 1 and 6 respectively, and do not cure the deficiencies of the parent claims in terms of being directed towards statutory subject matter. Therefore these claims are rejected on the same basis as claims 1 and 6.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent Documents teach timing attack countermeasures pertinent to the applicants disclosure.

Shamir	5,991,415
Reed et al.	5,600,324

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

1/20/05

Paul Gallaher

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER